INTERNATIONAL STANDARD

ISO 22316

First edition
2017-03

Security and resilience — Organizational resilience — Principles and attributes

Sécurité et résilience — Résilience organisationnelle — Principes et attributs

Reference number
ISO 22316:2017(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

Introduction

Organizational resilience is the ability of an organization to absorb and adapt in a changing environment to enable it to deliver its objectives and to survive and prosper. More resilient organizations can anticipate and respond to threats and opportunities, arising from sudden or gradual changes in their internal and external context. Enhancing resilience can be a strategic organizational goal, and is the outcome of good business practice and effectively managing risk.

An organization's resilience is influenced by a unique interaction and combination of strategic and operational factors. Organizations can only be more or less resilient; there is no absolute measure or definitive goal.

A commitment to enhanced organizational resilience contributes to:

— an improved ability to anticipate and address risks and vulnerabilities;

— increased coordination and integration of management disciplines to improve coherence and performance;

— a greater understanding of interested parties and dependencies that support strategic goals, and objectives.

There is no single approach to enhance an organization's resilience. There are established management disciplines that contribute towards resilience but, on their own, these disciplines are insufficient to safeguard an organization's resilience. Instead, organizational resilience is the result of the interaction of attributes and activities, and contributions made from other technical and scientific areas of expertise. These are influenced by the way in which uncertainty is addressed, decisions are made and enacted, and how people work together.

This document establishes the principles for organizational resilience. It identifies the attributes and activities that support an organization in enhancing its resilience.

This document includes:

— principles providing the foundation for enhancing an organization's resilience;

— attributes describing the characteristics of an organization that allow the principles to be adopted;

— activities guiding the utilization, evaluation and enhancement of attributes.

Security and resilience — Organizational resilience — Principles and attributes

1 Scope

This document provides guidance to enhance organizational resilience for any size or type of organization. It is not specific to any industry or sector. This document can be applied throughout the life of an organization.

This document does not promote uniformity in approach across all organizations, as specific objectives and initiatives are tailored to suit an individual organization's needs.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Societal security — Terminology*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
management
coordinated activities to direct and control an organization

3.2
interested party
person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: This can be an individual or group that has an interest in any decision or activity of an organization.

3.3
organizational culture
collective beliefs, values, attitudes and behaviour of an organization that contribute to the unique social and psychological environment in which it operates

3.4
organizational resilience
ability of an organization to absorb and adapt in a changing environment

3.5
values
beliefs an organization adheres to and the standards that it seeks to observe

4 Principles

4.1 General

The principles provide the foundation upon which a framework and strategy to achieve an enhanced state of organizational resilience can be developed, implemented and evaluated.

An organization's resilience:

a) is enhanced when behaviour is aligned with a shared vision and purpose;

b) relies upon an up-to-date understanding of an organization's context;

c) relies upon an ability to absorb, adapt and effectively respond to change;

d) relies upon good governance and management;

e) is supported by a diversity of skills, leadership, knowledge and experience;

f) is enhanced by coordination across management disciplines and contributions from technical and scientific areas of expertise;

g) relies upon effectively managing risk.

4.2 Coordinated approach

The organization should develop a coordinated approach that provides:

— a mandate to ensure its leaders and top management are committed to enhance organizational resilience;

— adequate resources needed to enhance the organization's resilience;

— appropriate governance structures to achieve the effective coordination of organizational resilience activities;

— mechanisms to ensure investments in resilience activities are appropriate to the organization's internal and external context;

— systems that support the effective implementation of organizational resilience activities;

— arrangements to evaluate and enhance resilience in support of organizational requirements;

— effective communications to improve understanding and decision making.

5 Attributes for organizational resilience

5.1 General

An organization that has adopted the resilience principles will demonstrate common attributes supported by activities, which guide their utilization, evaluation and enhancement. Such attributes include those described in 5.2 to 5.10.

5.2 Shared vision and clarity of purpose

Organizational resilience is enhanced by a clearly articulated and understood purpose, vision and values to provide clarity to decision making at all levels of the organization.

The organization should prioritize and resource the following activities:

a) articulate its vision, purpose and core values to all interested parties to provide strategic direction, coherence and clarity in all decision-making;

b) ensure individual goals and objectives are aligned with and committed to the organization's purpose, vision and values;

c) monitor and review regularly the suitability of the organization's strategies and their alignment with purpose, vision, core values and objectives;

d) recognize the need to reflect on and, if necessary, revise the organization's purpose, vision and core values in response to external and internal changes;

e) seek out and promote new and innovative ideas to achieve and develop its strategic objectives.

5.3 Understanding and influencing context

A comprehensive understanding of the organization's internal and external environments will help the organization make more effective strategic decisions about the priorities for resilience.

The organization should demonstrate and enhance the following:

— the ability to think beyond current activities, strategy, and organizational boundaries;

— understanding, collaborating and strengthening of relationships with relevant interested parties to support the delivery of the organization's purpose and vision.

The organization should prioritize and resource the following activities:

a) monitor and evaluate the organization's context, including interdependencies, political, regulatory environment and competitor activities under changing circumstances;

b) maintain strong relationships with interested parties and foster co-operation at all levels;

c) collaborate with interested parties that share the organization's purpose and vision.

5.4 Effective and empowered leadership

Organizational resilience is enhanced by leadership that develops and encourages others to lead under a range of conditions and circumstances, including during periods of uncertainty and disruptions.

The organization should demonstrate and enhance the following:

— effective leadership throughout the organization that encourages a culture supportive of resilience;

— leadership that can adapt to changing circumstances;

— leadership that utilizes a diverse set of skills, knowledge and behaviour within the organization to achieve organizational objectives.

The organization should prioritize and resource the following activities:

a) develop trusted and respected leaders who act with integrity and are committed to a sustained focus on organizational resilience;

b) assign roles and responsibilities for enhancing organizational resilience;

c) encourage the creation and sharing of lessons learned about success and failure and promote the adoption of better practice;

d) empower all levels of the organization to make decisions that protect and enhance the resilience of the organization.

5.5 A culture supportive of organizational resilience

A culture that is supportive of organizational resilience demonstrates a commitment to, and existence of, shared beliefs and values, positive attitudes and behaviour.

The organization should prioritize and resource the following activities:

a) determine the beliefs, values and behaviour within the organization that define organizational culture;

b) identify core values and behaviour that enhance organizational resilience and establish criteria that can be applied to assess individual performance;

c) engage people at all levels to promote the organization's values;

d) foster creativity and innovation that enhances organizational resilience;

e) empower people to identify and communicate threats and opportunities and to take action that will benefit the organization;

f) monitor and review organizational culture to detect any changes that may influence organizational resilience.

5.6 Shared information and knowledge

Organizational resilience is enhanced when knowledge is widely shared where appropriate and applied. Learning from experience and learning from each other is encouraged.

The organization should demonstrate and enhance the following:

— information, knowledge, and learning is valued;

— learning is drawn from all available sources (uses what it has and learns from others).

The organization should ensure that knowledge and information is:

a) accessible, understandable and adequate to support the organization's objectives;

b) effectively shared to enable decision-making;

c) recognized as a critical resource of the organization;

d) created, retained and applied through established systems and processes;

e) shared in a timely manner with all relevant interested parties;

f) applied in organizational learning.

5.7 Availability of resources

The organization should develop and allocate resources, such as people, premises, technology, finance and information, to address vulnerabilities, providing the ability to adapt to changing circumstances.

The organization should prioritize and resource the following activities:

a) take appropriate decisions on resourcing and capacity, diversification, replication and redundancy to avoid single points of failure and respond to incidents and change, so that core services are maintained at an acceptable, pre-determined level;

b) select and develop employees with a diverse set of skills, knowledge and behaviour that can contribute to the organization's ability to respond and adapt to change;

c) develop an ability to identify and respond to change in a flexible manner; including modifying and redeploying capabilities, arrangements, structures, activities and behaviour to adjust to new conditions;

d) routinely review the suitability, availability and allocation of resources, taking account of the impact of any changes in the organization and its context.

5.8 Development and coordination of management disciplines

The design, development and coordination of management disciplines and their alignment with the organization's strategic objectives are fundamental to enhancing organizational resilience.

NOTE Annex A provides a sample list of management disciplines.

The organization should demonstrate and enhance the following:

— the management disciplines are coordinated so that they individually and collectively contribute to the organization's purpose and the protection of what it values;

— the organization manages the effect of uncertainty on its objectives across management disciplines.

The organization should prioritize and resource the following activities:

a) identify and design management disciplines that contribute toward the organization's resilience;

b) regularly assess how each management discipline contributes to the overall resilience of the organization, and address weaknesses where these are found;

c) build flexibility into the management disciplines so that the organization can absorb and adapt to change;

d) enhance communication, coordination, and cooperation between management disciplines of the organization to build a coherent approach.

5.9 Supporting continual improvement

Organizational resilience is improved when organizations continually monitor their performance against pre-determined criteria to learn and improve from experience and take advantage of opportunities. Organizations create and encourage a culture of continual improvement across all employees.

The organization should demonstrate and enhance the following:

— a culture of continual improvement that ensures organizational objectives, strategies and procedures can be kept relevant and appropriate in supporting the changing needs of the organization;

— a commitment to validate and continually improve organizational resilience activities and capabilities.

The organization should prioritize and resource the following activities:

a) implement performance monitoring and evaluation mechanisms to support continual improvement;

b) ensure that performance management criteria are responsive to changes that impact on organizational objectives.

5.10 Ability to anticipate and managing change

Organizational resilience is enhanced when an organization has the ability to anticipate, plan, and respond to change.

The organization should demonstrate and enhance the following:

— the ability to deliver consistently on its commitments under changing circumstances and adapting its operations accordingly;

— the ability to absorb and adapt to the impacts of sudden and unexpected incidents;

— preparation to respond to change, or influence change if necessary.

The organization should prioritize and resource the following activities:

a) remain aware of situations that are likely to influence change;

b) adapt itself when needed without significant impact to its products and services;

c) commit to protection, performance and adaptation but with the ability to shift focus without compromising its visions and core values;

d) ensure that the management disciplines are sufficiently robust and effective to respond to changes.

6 Evaluating the factors that contribute to resilience

6.1 General

Evaluation activities provide intelligence and management information on how strategies and objectives for organizational resilience continue to meet the needs of the organization, or where there are opportunities for improvement.

The organization should:

— establish processes to allow it to continuously measure and monitor the factors that contribute to organizational resilience as an aid to management decisions;

— target measurement and monitoring activities to the specific attributes of the organization that enhance its resilience;

— evaluate the effectiveness of its resilience approach and objectives against these attributes.

6.2 Organizational requirements

6.2.1 General

Performance measures used in the evaluation process are likely to be selected on the basis of the sector in which the organization operates, the criteria determined by top management and the organizational culture.

Most organizations already collect performance data that can be applied to an assessment of their resilience. Sources may include existing management information and internal audit reports, business review processes and project reporting.

Top management should:

— determine the appropriate objectives for organizational resilience;

— develop measurement criteria to be used to monitor and evaluate the status of the organization‘s resilience attributes;

— monitor and evaluate the organization’s overall resilience maturity and performance;

— identify what needs to be evaluated and monitored, and the methods that will produce valid results and a continuous assessment of organizational resilience;

— determine the thresholds at which the output from the evaluation will be considered acceptable;

— decide how evaluation and monitoring arrangements will parallel, support or be integrated into existing monitoring processes;

— establish how the results from monitoring and measurement will be analysed, evaluated and reported.

6.2.2 Determining gaps

The initial assessment of organizational resilience can be used to inform any work that is required urgently, and reinforce the concept of organizational resilience with interested parties.

The organization should:

— undertake a review, applying the agreed metrics to determine the organization's resilience before implementing a monitoring process;

— determine if resilience is acceptable to top management or falls short of the organization's requirements;

— consider appropriate strategies to address any significant gaps that are found in the assessment.

6.3 Monitoring and assessment

6.3.1 Methods and processes

Monitoring and assessing organizational resilience helps to identify the signs of an emerging issue or an opportunity that requires attention. Failure to identify these signs could limit an organization's ability to address issues before they have an impact, and could limit the effectiveness and increase the costs of any mitigating actions.

The organization should:

— apply existing monitoring methods and processes to evaluate attributes that contribute to their resilience;

— monitor the effectiveness of initiatives established for the management of risk, including those managed by established management disciplines;

— consider the use of employee and customer surveys that provide indicators of resilience within the organization;

— seek to understand what data are required to make an assessment of resilience and ensure there is an evaluation process to support this.

6.3.2 Review

Top management should carry out a periodic review to ensure the organization's resilience continues to meet expectations. The review should consider changes in the organization's context, including:

— changes in organizational vision, strategy or objectives;

— major structural or business model changes, including mergers, acquisitions and divestments;

— new markets or territories that the organization has entered;

— newly introduced products and services;

— significant staff changes, including top management;

— the effectiveness of improvements made since the previous review;

— feedback on the effectiveness of the organization's resilience;

— change in risks that need to be addressed.

Top management should:

— compare the outputs from the organizational resilience evaluation process against other related review processes, such as the results from related internal audits, incident debriefs, strategy planning, near misses and regulatory compliance;

— confirm that monitoring arrangements are appropriate and provide input to the identification and treatment of issues before their impacts become too damaging or an opportunity is missed.

6.4 Reporting

The outputs from monitoring organizational resilience may include summary reporting, giving top management an assessment of resilience against the attributes most relevant to the organization.

Top management should:

— use on-going monitoring reports to track trends in the data that have been used to evaluate organizational resilience;

— confirm that current information management systems provide essential data to support the input required for an organization's resilience monitoring;

— use the output of the reporting process to develop action plans to enhance organizational resilience.

Annex A
(informative)

Relevant management disciplines

Management disciplines that can support the guidance given in 5.8 include the following:

— asset management;

— business continuity management;

— crisis management;

— cyber security management;

— communications management;

— emergency management;

— environmental management;

— facilities management;

— financial control;

— fraud control;

— governance;

— health and safety management;

— human resources management;

— information security management;

— information, communications and technology;

— physical security management;

— quality management;

— risk management;

— supply chain management;

— strategic planning.

Bibliography

[1] ISO 22301, *Societal security — Business continuity management systems --- Requirements*

[2] ISO 22398, *Societal security — Guidelines for exercises*

[3] ISO 31000, *Risk management — Principles and guidelines*

[4] ISO/IEC 38500, *Information technology — Governance of IT for the organization*

[5] ISO Guide 73, *Risk management — Vocabulary*